MATHEMATICS OF COMPUTATION

TABLE OF CONTENTS

July 1993

Leonard M. Adleman and Jonathan DeMarrais, A subexponential algorithm for discrete logarithms over all finite fields 1

Walter Aiello and M. V. Subbarao, A conjecture in addition chains related to Scholz's conjecture 17

Tom M. Apostol, An extension of the Lehmers' picturesque exponential sums 25

A. O. L. Atkin and F. Morain, Elliptic curves and primality proving..... 29

Eric Bach and Lorenz Huelsbergen, Statistical evidence for small generating sets 69

Richard Blecksmith, John Brillhart, and Irving Gerst, A fundamental modular identity and some applications 83

Wieb Bosma, Explicit primality criteria for $h \cdot 2^k \pm 1$ 97

Andrew Bremner and Duncan A. Buell, Three points of great height on elliptic curves 111

Andrew Bremner, Richard K. Guy, and Richard J. Nowakowski, Which integers are representable as the product of the sum of three integers with the sum of their reciprocals? 117

Richard P. Brent, On computing factors of cyclotomic polynomials 131

J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, Irregular primes and cyclotomic invariants to four million 151

Harvey Cohn, How branching properties determine modular equations .. 155

T. W. Cusick, Zaremba's conjecture and sums of the divisor function ... 171

Ivan Damgård, Peter Landrock, and Carl Pomerance, Average case error estimates for the strong probable prime test 177

J.-M. Deshouillers and F. Dress, Numerical results for sums of five and seven biquadrates and consequences for sums of 19 biquadrates ... 195

Jean-Marc Deshouillers, Andrew Granville, Władysław Narkiewicz, and Carl Pomerance, An upper bound in Goldbach's problem 209

P. Erdős, C. B. Lacampagne, and J. L. Selfridge, Estimates of the least prime factor of a binomial coefficient 215

Tom Hansen, Gary L. Mullen, and Harald Niederreiter, Good parameters for a class of node sets in quasi-Monte Carlo integration 225

D. R. Heath-Brown, W. M. Lioen, and H. J. J. te Riele, On solving the Diophantine equation $x^3 + y^3 + z^3 = k$ on a vector computer 235

D. A. Hejhal and S. Arno, On Fourier coefficients of Maass waveforms for $\mathrm{PSL}(2, \mathbf{Z})$ 245

Marvin I. Knopp, On the cuspidal spectrum of the arithmetic Hecke groups 269

Donald E. Knuth, Johann Faulhaber and sums of powers 277

Andrew J. Lazarus, Cyclotomy and delta units 295

D. H. Lehmer, The mathematical work of Morgan Ward 307

D. H. Lehmer and Emma Lehmer, The Lehmer project 313
A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, The factorization of the ninth Fermat number 319
H. W. Lenstra, Jr. and J. O. Shallit, Continued fractions and linear recurrences 351
R. A. Mollin, Ambiguous classes in quadratic fields 355
Peter L. Montgomery, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ 361
Joseph B. Muskat, Generalized Fibonacci and Lucas sequences and rootfinding methods 365
Andrew M. Odlyzko, Iterated absolute values of differences of consecutive primes 373
R. G. E. Pinch, The Carmichael numbers up to 10^{15} 381
Raphael M. Robinson, Numbers having m small mth roots mod p 393
Robert Rumely, Numerical computations concerning the ERH 415
A. Schinzel, An extension of the theorem on primitive divisors in algebraic number fields 441
Robert D. Silverman and Samuel S. Wagstaff, Jr., A practical analysis of the elliptic curve factoring algorithm 445
H. C. Williams, How was F_6 factored? 463
Kenneth S. Williams and Kenneth Hardy, A refinement of H. C. Williams' qth root algorithm 475
D. Zagier, Algebraic numbers close to both 0 and 1 485
Supplement to "A conjecture in addition chains related to Scholz's conjecture" by **Walter Aiello and M. V. Subbarao** S1
Supplement to "Explicit primality criteria for $h \cdot 2^k \pm 1$" by **Wieb Bosma** S7
Supplement to "On Fourier coefficients of Maass waveforms for PSL(2, $\mathbb{Z}$)" by **D. A. Hejhal and S. Arno** S11
Supplement to "Numerical computations concerning the ERH" by **Robert Rumely** S17

TABLE OF CONTENTS

October 1993

Harald Berger and Miloslav Feistauer, Analysis of the finite element variational crimes in the numerical approximation of transonic flow ... 493
John W. Barrett and W. B. Liu, Finite element approximation of the p-Laplacian 523
Lucia Gastaldi, Uniform interior error estimates for the Reissner-Mindlin plate model 539
Charalambos G. Makridakis, Finite element approximations of nonlinear elastic waves 569

Dongwoo Sheen, Second-order absorbing boundary conditions for the wave equation in a rectangular domain 595
Gui-Qiang Chen and Jian-Guo Liu, Convergence of second-order schemes for isentropic gas dynamics 607
Gui-Qiang Chen, Qiang Du, and Eitan Tadmor, Spectral viscosity approximations to multidimensional scalar conservation laws 629
Pravir K. Dutt and A. K. Singh, Spectral methods for periodic initial value problems with nonsmooth data 645
G.-H. Cottet and L. Germain, Image processing through reaction combined with nonlinear diffusion 659
Paul Muir and Brynjulf Owren, Order barriers and characterizations for continuous mono-implicit Runge-Kutta schemes 675
Man-Chung Yeung and Raymond H. Chan, Circulant preconditioners for Toeplitz matrices with piecewise continuous generating functions .. 701
Ivo Marek and Daniel B. Szyld, Iterative and semi-iterative methods for computing stationary probability vectors of Markov operators 719
G. Alefeld, F. A. Potra, and Yixun Shi, On enclosing simple roots of nonlinear equations 733
Knut S. Eckhoff, Accurate and efficient reconstruction of discontinuous functions from truncated series expansions 745
Walter Van Assche and Ingrid Vanherwegen, Quadrature formulas based on rational interpolation 765
H. Brass, Asymptotically optimal error bounds for quadrature rules of given degree 785
J. N. Lyness and T. Sørevik, Lattice rules by component scaling 799
Stephen Joe, Bounds on the lattice rule criterion R 821
Michael Clausen and Ulrich Baum, Fast Fourier transforms for symmetric groups: theory and implementation 833
Bert van Geemen and Duco van Straten, The cusp forms of weight 3 on $\Gamma_2(2,4,8)$ 849
Johannes Buchmann, David Ford, and Michael Pohst, Enumeration of quartic fields of small discriminant 873
Kurt Girstmair, The relative class numbers of imaginary cyclic fields of degrees 4, 6, 8, and 10 881
Meinolf Geck, The decomposition numbers of the Hecke algebra of type E_6^* 889
M. Mignotte and N. Tzanakis, Arithmetical study of a certain ternary recurrence sequence and related questions 901
Gerhard Jaeschke, On strong pseudoprimes to several bases 915
Harvey Dubner, Generalized repunit primes 927
Matti K. Sinisalo, Checking the Goldbach conjecture up to $4 \cdot 10^{11}$ 931
David Moews and Paul C. Moews, A search for aliquot cycles and amicable pairs 935

Reviews and Descriptions of Tables and Books 939
Lambert **35**, Dongarra, Kennedy, Messina, Sorensen, and Voigt, Editors **36**, Daubechies **37**, Korneichuk **38**, Hagen, Editor **39**, Hagen, Editor **40**, Naudin and Quitté **41**, Moews and Moews **42**
Supplement to "The relative class numbers of imaginary cyclic fields of degrees 4, 6, 8, and 10" by **Kurt Girstmair** S25